Załącznik nr 1

WYMAGANIA
NA
MODUŁ OPROGRAMOWANIA

ENIGMA SYSTEMY OCHRONY INFORMACJI SP. Z O.O.
JUTRZENKI 116
02-230 WARSZAWA
POLSKA

TELEFON: +48 22 570 57 10
FAX: +48 22 570 57 15
STRONA INTERNETOWA: WWW.ENIGMA.COM.PL

DOKUMENT STWORZONY PRZEZ

ENIGMA SYSTEMY OCHRONY INFORMACJI SP. Z O.O.
02-230 WARSZAWA, UL. JUTRZENKI 116 | TELEFON: +48 22 570 57 10 | FAX: +48 22 570 57 15

SPIS TREŚCI

1 WSTĘP

Dokument przedstawia technologiczne, niefunkcjonalne i funkcjonalne wymagania dla modułu oprogramowania realizującego następujące usługi:

- obsługi użytkowników;
- zarządzania grupami uprawnień;
- uwierzytelniania.

2 SPECYFIKACJA WYMAGAŃ

2.1 WYMAGANIA NIEFUNKCJONALNE

2.1.1 ARCHITEKTURA/KOMUNIKACJA

1. Architektura modułu musi być oparta na mikrousługach - małych, modularnych i luźno powiązanych serwisach, gdzie każdy serwis wykonuje unikalny proces lub jego fragment.
2. Komunikacja synchroniczna między serwisami musi odbywać się za pomocą lekkiego mechanizmu HTTPS REST/JSON.
3. Komunikacja asynchroniczna między serwisami musi odbywać się za pośrednictwem brokera wiadomości Apache Kafka.
4. Dla publicznych interfejsów usług muszą zostać dostarczone biblioteki języka Java realizujące komunikację z tymi interfejsami.

2.1.2 WYKORZYSTYWANE TECHNOLOGIE

1. Komponenty muszą być zrealizowane w języku Java lub Kotlin.
2. Komponenty muszą wykorzystywać framework Spring Boot.

2.1.3 ŚRODOWISKO URUCHOMIENIOWE

1. Komponenty muszą zapewniać współpracę z oprogramowaniem serwerowym Linux.
2. Dla każdej mikrousługi musi zostać dostarczony obraz zgodny z narzędziem, do wirtualizacji na poziomie systemu operacyjnego, Docker w wersji 19.03 lub nowszej.

3. Mikrousługi wymagające relacyjnej bazy danych, muszą być kompatybilne z PostgreSQL w wersji 9.6 lub nowszej.
4. Mikrousługi wymagające bazy danych typu klucz-wartość, muszą być kompatybilne z Redis w wersji 4.0 lub nowszej.

2.2 WYMAGANIA FUNKCJONALNE NA MODUŁ OPROGRAMOWANIA

2.2.1 KOMPONENT OBSŁUGI UŻYTKOWNIKÓW (KOU)

IDENTYFIKATOR	FUNKCJONALNOŚĆ
KOU.1.	Komponent umożliwia tworzenie kont Użytkowników.
KOU.2.	Konto posiada pola: a) login, b) imię, c) nazwisko, d) status, e) hasło.
KOU.3.	Komponent nie przechowuje haseł użytkowników, a jedynie wyniki funkcji skrótu z haseł.
KOU.4.	Komponent umożliwia blokowanie i odblokowywanie użytkowników.
KOU.5.	Komponent umożliwia edycję kont Użytkowników.
KOU.6.	Komponent umożliwia zmianę hasła użytkownika. Ustawienie nowego hasła wymaga podanie bieżącego hasła.
KOU.7.	Komponent umożliwia resetowania hasła przy pomocy odnośnika wysyłanego na adres e-mail użytkownika.
KOU.8.	Komponent umożliwia pobranie stronicowanej listy kont z możliwością filtrowania. Dostępne są filtry: a) zbiór identyfikatorów, b) tekst (dopasowanie do imienia, nazwiska, adresu email), c) wartość określającą czy konto jest zablokowane.
KOU.9.	Komponent umożliwia wymuszenie złożoności hasła: liczba wymaganych wielkich liter.
KOU.10.	Komponent umożliwia wymuszenie złożoności hasła: liczba wymaganych małych liter.
KOU.11.	Komponent umożliwia wymuszenie złożoności hasła: liczba wymaganych znaków specjalnych.
KOU.12.	Komponent umożliwia wymuszenie złożoności hasła: liczba wymaganych cyfr (0-9).
KOU.13.	Komponent umożliwia wymuszenie złożoności hasła: możliwość tworzenia listy zakazanych znaków.
KOU.14.	Komponent umożliwia zdefiniowanie minimalnej długości hasła.
KOU.15.	Komponent udostępnia możliwość wymuszenia zmiany hasła przez użytkownika po jego resecie.
KOU.16.	Komponent umożliwia pobranie pojedynczego konta po jego identyfikatorze.
KOU.17.	Użytkownik przypisany jest do jednostki organizacyjnej.
KOU.18.	Użytkownik przypisany jest do grup uprawnień powiązanych z jednostką organizacyjną.

KOU.19.	Komponent umożliwia wykonywanie następujących operacji na jednostkach organizacyjnych tworzących strukturę organizacyjną: a) tworzenie, b) edycja, c) usuwanie.
KOU.20.	Komponent umożliwia zarządzanie użytkownikami oraz grupami uprawnień w ramach jednostki organizacyjnej.
KOU.21.	System umożliwia obsługę hierarchicznego powiązania pomiędzy jednostkami organizacyjnymi
KOU.22.	Komponent umożliwia usuwanie kont Użytkowników.
KOU.23.	Komponent umożliwia edycję statusu konta Użytkownika.
KOU.24.	Komponent umożliwia anonimizację danych Użytkownika.
KOU.25.	Komponent posiada wsparcie do obsługi wymagań RODO.
KOU.26.	Komponent udostępnia graficzny interfejs użytkownika, realizujący wymienione funkcje.
KOU.27.	Komponent umożliwia podgląd Użytkowników aktualnie zalogowanych.
KOU.28.	Komponent umożliwia audytowanie wszystkich prób dostania się do danych i ich modyfikacji.
KOU.29.	Komponent umożliwia obsługę hierarchicznego powiązania pomiędzy jednostkami organizacyjnymi.
KOU.30.	Komponent umożliwia obsługę zmian organizacyjnych, pilnowanie przyporządkowania pracowników do struktury organizacyjnej.
KOU.31.	Komponent umożliwia synchronizację kont użytkowników z usługą katalogową LDAP (Lightweight Directory Access Protocol).

2.2.2 KOMPONENT GRUP UPRAWNIEŃ (KGU)

IDENTYFIKATOR	FUNKCJONALNOŚĆ
KGU.1.	Komponent umożliwia wykonywanie następujących operacji na grupach uprawnień do funkcji biznesowych: a) tworzenie, b) edycja, c) usuwanie.
KGU.2.	Komponent umożliwia tworzenie grup systemowych, które są zablokowane do edycji dla Administratora Systemu.
KGU.3.	Komponent umożliwia przypisanie Użytkownika do grup w ramach struktury organizacyjnej, z których będzie dziedziczył uprawnienia. Jeśli Użytkownik jest przypisany do kilku grup uprawnienia będą sumą logiczną uprawnień z wszystkich grup, do których Użytkownik należy.
KGU.4.	Komponent umożliwia kopiowanie grup uprawnień.
KGU.5.	Komponent udostępnia graficzny interfejs użytkownika, realizujący wymienione funkcje.
KGU.6.	Komponent umożliwia audytowanie wszystkich prób dostania się do danych i ich modyfikacji.

2.2.3 KOMPONENT UWIERZYTELNIENIA (KU)

IDENTYFIKATOR	FUNKCJONALNOŚĆ
KU.1.	Komponent umożliwia logowanie użytkownikom, którzy nie zostali zablokowani.
KU.2.	Operacja logowania zwraca token dostępowy i token do odświeżania tokena dostępowego.
KU.3.	Token dostępowy wygasa po określonym czasie.
KU.4.	Komponent umożliwia wylogowanie - unieważnienie wystawionych tokenów.
KU.5.	Komponent umożliwia odświeżanie tokena dostępowego za pomocą ważnego tokena odświeżającego.
KU.6.	Konto użytkownika blokowane jest po określonej liczbie błędnie wpisanego hasła.
KU.7.	Komponent umożliwia obsługę tokenów użytkownika przypisanych do poszczególnych aplikacji klienckich.
KU.8.	Komponent udostępnia graficzny interfejs użytkownika, realizujący wymienione funkcje.
KU.9.	Komponent umożliwia automatyczne rozłączenie sesji po zadanym czasie nieaktywności Użytkownika.

2.3 WYMAGANIA LICENCYJNE

Ze względu na wymagania Narodowego Centrum Badań i Rozwoju w zakresie praw własności intelektualnej w projektach na rzecz obronności i bezpieczeństwa Państwa przedmiot dostawy musi spełniać następujące wymagania licencyjne:

- Licencjobiorcą zostaje Enigma Systemy Ochrony Informacji Sp. z o.o.
- Producent oprogramowania oświadcza, że posiada prawo do udzielenia licencji na Oprogramowanie i Dokumentację w zakresie określonym Umową.
- Producent oprogramowania udziela Licencjobiorcy licencji na Oprogramowanie i Dokumentację w zakresie określonym Umową. Licencja jest pełna, niewyłączna i udzielona na czas nieograniczony. Nieograniczony jest również zasięg terytorialny licencji. Okres wypowiedzenia licencji wynosi 20 lat.
- Licencjobiorca ma prawo udzielenia dalszej licencji podmiotom trzecim.
- Producent oprogramowania udziela Licencjobiorcy licencji na użytkowanie Oprogramowania i Dokumentacji w zakresie niezbędnym do swobodnego korzystania z systemu HIT-NET i rozporządzania nim na wszystkich polach eksploatacji znanych w chwili zawarcia Umowy.